Abstract of the Disclosure

Systems and methods are provided for performing digital signing and encryption using identity-based techniques. A message may be signed and encrypted in a single operation and may be decrypted and verified in two separate operations. Messages may be sent anonymously and confidentially. The systems and methods support message confidentiality, signature non-repudiation, and ciphertext authentication, ciphertext unlinkability, and anonymity.